UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,453	08/14/2001	Graeme John Proudler	B-4276PCT 619003-1	9595

7590 06/29/2005

IP Administration
Hewlett Packard Company
3404 East Harmony Road
Mail Stop 35
Ft Collins, CO 80528-9599

EXAMINER	
PHAN, TRI H	

ART UNIT	PAPER NUMBER
2661	

DATE MAILED: 06/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/913,453	PROUDLER ET AL.	
	Examiner	Art Unit	
	Tri H. Phan	2661	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 August 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1-4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This Office Action is in response to the Amendment filed on August 14th, 2001. New claims 21-30 are added. Claims 1-30 are now pending in the application.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

3. The drawings are objected to because all blocks in Figures 1-3 should be labeled with descriptive legends based on 37 C.F.R. § 1.84(o) for supporting the objection in the Rules and M.P.E.P. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 4, 14-16 and 24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 4, it recites the limitation "... which can and/or cannot be permitted ..." is vague and indefinite because the phrase "which can and cannot be permitted" appears to be negative statement which would renders the claim indefinite.

Similar problems exist in claim 15, line 3 and claim 24, line 3; wherein the limitation "... which can and/or cannot be permitted ..." is vague and indefinite because the phrase "which can and cannot be permitted" appears to be negative statement which would renders the claim indefinite.

In regard to claim 14, line 8, the term "may be" is vague and indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention or not, and the resulting claim does not clearly set forth the metes and bounds of the patent protection desired.

Similar problem exists in claim 16, lines 5, 8 and 9, the term "may be" is vague and indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention or not, and the resulting claim does not clearly set forth the metes and bounds of the patent protection desired.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-3, 5-6, 13, 18, 21-23 and 25-26 are rejected under 35 U.S.C. 102(b) as being anticipated by **Boebert et al.** (U.S.5,822,435; hereinafter refer as '**Boebert**').

- In regard to claims 1 and 21, **Boebert** discloses in Figs. 1-6 and in the respective portions of the specification about *the computing apparatus* (For example see Fig. 2; Abstract; col. 3, lines 20-40; col. 4, lines 33-39), *which comprises the trusted hardware module* ("trusted path subsystem"; For example see Figs. 2-4; col. 4, lines 33-39) *resistant to unauthorized modification* (For example see col. 2, lines 27-38), *a plurality of further hardware modules* ("workstation processing unit, display with video manager, keyboard with keyboard manager"; For example see Figs. 1-4), *the shared communication infrastructure* ("paths 44, 46" which connect the workstation processing unit to the display/video manager, keyboard/keyboard manager) *by which the hardware modules can communicate with each other* (For example see Figs. 1-4; col. 2, lines 1-4; wherein the workstation processing unit communicates directly with the display/video manager, keyboard/keyboard manager) *and the first communication path distinct from the shared communication infrastructure* ("separate data path" or "auxiliary data path"; For example see Figs. 3-4; col. 4, lines 33-39), *by which the first one of the further*

hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules (For example see Figs. 3-4; col. 4, lines 33-50; wherein the workstation processing unit communicates with display/video manager, keyboard/keyboard manager through the trusted path subsystem).

- Regarding claims 2 and 22, in addition to features in base claims 1 and 21 (see rationales pertaining the rejection of base claims 1 and 21 discussed above), **Boebert** further discloses *wherein the trusted hardware module* ("trusted path subsystem") *and the first further hardware module* ("workstation processing unit") *each include a respective computing engine* ("processor"; For example see Figs 3-4; wherein it is inherent that the workstation processing unit has its own processor for processing the application for the workstation unit) *which partakes in the direct communication via the first communication path.*

- In regard to claims 3 and 23, in addition to features in base claims 1 and 21 (see rationales pertaining the rejection of base claims 1 and 21 discussed above), **Boebert** further discloses *wherein the first further hardware module is operable to supply to the trusted hardware module the request for operation on data* ("trusted path mode"; For example see col. 5, lines 17-32; wherein the workstation invokes trusted path mode through different number of ways as disclosed in col. 5, line 66 through col. 6, line 10; e.g. '*request for operation on data*') *and in response to such a request, the trusted hardware module is operable to generate a response* ("feedback mechanism"; For example see col. 6, lines 8-10) *and to supply the response*

to the first further hardware module via the first communication path and not via the shared communication infrastructure (For example see Figs. 3-4; col. 5, lines 27-32).

- Regarding claims 5-6 and 25-26, in addition to features in base claims 1 and 21 (see rationales pertaining the rejection of base claims 1 and 21 discussed above), **Boebert** further discloses *wherein the trusted hardware module is operable to generate an encryption and/or decryption key* ("pair-wise key" or "public key") *and supply that key to the first further hardware module via the first communication path and not via the shared communication infrastructure* (For example see col.5, lines 52-65); *and wherein the first further hardware module is operable to use the key for encryption and/or decryption of data communicated via the shared communication infrastructure* (For example see col. 4, line 51 through col. 5, line 2).

- In regard to claims 13 and 18, in addition to features in base claims 1 and 21 (see rationales pertaining the rejection of base claims 1 and 21 discussed above), **Boebert** further discloses about the second and third communication paths, distinct from the shared communication infrastructure and the first communication path, by which the second one of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules ("*second and third communication paths*"; For example see Figs. 3-4; wherein the display and keyboard connect to the video and keyboard managers, and then connect to the multi-level secure computer via network interface 39 and network 50).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 4, 7-12, 14-17, 19-20, 24 and 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Boebert et al.** (U.S.5,822,435; hereinafter refer as '**Boebert**')..

- In regard to claims 4 and 24, **Boebert** discloses all the subject matter of the claimed invention as discussed above about *the computing apparatus* (For example see Fig. 2), *which comprises the trusted hardware module* ("trusted path subsystem"; For example see Figs. 2-4) *resistant to unauthorized modification, a plurality of further hardware modules* ("workstation processing unit, display with video manager, keyboard with keyboard manager"; For example see Figs. 1-4), *the shared communication infrastructure* ("paths 44, 46") *by which the hardware modules can communicate with each other and the first communication path distinct from the shared communication infrastructure* ("separate data path" or "auxiliary data path"), *by which the first one of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules* (For example see Figs. 3-4); including the storage device ('*means for storing*') and the capable of recognizing classified information of varying sensitivity and different levels of users access of the multi-level secure computer (For example see Figs. 1-2; col. 1, lines 20-27; col. 2,

lines 15-25; col. 7, lines 27-44). Though, **Boebert** does not explicitly disclose about "*policy information*"; however, in order to recognizing classified information of varying sensitivity and different levels of users access, the multi-level secure 'MLS' computer (see Figs. 1-2) has to store information about different levels to access to the secure subsystem, e.g. "*policy information*", to provide the access right to users.

- Regarding claims 7-8, 20, 27-28 and 30, in addition to features in base claims 1 and 21 (see rationales pertaining the rejection of base claims 1 and 21 discussed above), **Boebert** further discloses *wherein the trusted hardware module is operable to generate a challenge and to supply the challenge to the first further hardware module via the first communication path or via the shared communication infrastructure using encryption set up using the first communication path* (For example see col. 6, lines 26-39; wherein, in order to access the system, the user from the workstation has to authenticated himself to the secure subsystem, where the "*challenge*" from the subsystem such as the login window is obvious and well known in the art); *and wherein, in response to the challenge, the first further hardware module is operable to generate a response and to supply the response the trusted hardware module via the first communication path the shared communication infrastructure using encryption set up using the first communication path* (For example see col. 6, lines 26-39; wherein the user provides the personal identification number 'PIN', password, biometric or token device to authenticate himself to the subsystem in order to access the secure system). Though, **Boebert** does not explicitly disclose about "*integrity metric*"; however, it is obvious that information such as personal identification number 'PIN', password, biometric or token device are used to authenticate the user to the secure subsystem and

are the "*integrity metric*", which create and store by the trusted system, in order to provide classified information of varying sensitivity and different levels of users access right for different user.

Thus it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the implementation "*integrity metric*" into the **Boebert**'s trusted subsystem, with the motivation being to provide classified information of varying sensitivity and different levels of users access right for different user.

- In regard to claims 9-12 and 29, in addition to features in base claim 1 (see rationales pertaining the rejection of base claim 1 discussed above), **Boebert** does discloses about the trusted ("*zone for private data*") and untrusted subsystem ("*zone for non-private data*") in the multi-level secure computer (For example see Figs. 1-2); and wherein the workstation has different levels of security (For example see col. 6, line 60 through col. 7, line 12) and different paths ("*network interface module*"; For example see Figs. 3-4) for receiving/transmitting data on normal mode, e.g. "*non-private data*" or non-secure, and trusted path mode, e.g. "*private data*" or secure (For example see Figs. 3-4); but fails to explicitly disclose about the different zones for receiving/transmitting data on normal mode and trusted path mode. However, it is obvious that configuring different "*zones*" for "*private data*" and "*non-private data*" is just system engineering choices to provide secure on transmitting or receiving data from different zones with different levels of security.

Thus it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the implementation the different zones for different levels of

security for the **Boebert**'s secure system, in order to provide secure on transmitting or receiving data from different zones with different levels of security.

- Regarding claims 14-16, in addition to features in base claim 1 (see rationales pertaining the rejection of base claim 1 discussed above), **Boebert** does discloses *wherein the first further hardware module is operable to supply to the trusted hardware module a request for a transfer of data between the first and second further hardware modules* ("trusted path mode"; For example see col. 5, lines 17-32; wherein the workstation invokes trusted path mode through different number of ways as disclosed in col. 5, line 66 through col. 6, line 10; e.g. '*request for a transfer of data*') *and in response to such a request, the trusted hardware module is operable to generate a response* ("feedback mechanism"; For example see col. 6, lines 8-10) *and to supply the response to the first or second further hardware module via the first or second communication path, not via the shared communication infrastructure* (For example see Figs. 3-4; col. 5, lines 27-32); including the storage device ('*means for storing*') and the capable of recognizing classified information of varying sensitivity and different levels of users access of the multi-level secure computer (For example see Figs. 1-2; col. 1, lines 20-27; col. 2, lines 15-25; col. 7, lines 27-44). Though, **Boebert** does not explicitly disclose about "*policy information*" as claimed in the claim invention 15; however, in order to recognizing classified information of varying sensitivity and different levels of users access, the multi-level secure 'MLS' computer (see Figs. 1-2) has to store information about different levels to access to the secure subsystem, e.g. "*policy information*", to provide the access right to users; and *wherein the trusted hardware module is operable to relay the data to the second or first further hardware module via the*

second or first communication path as claimed in the claim invention 16 (For example see col. 6, lines 34-39).

- In regard to claims 17 and 19, in addition to features in base claim 1 (see rationales pertaining the rejection of base claim 1 discussed above), **Boebert** further discloses about the processor ("*main processor*"; For example see Figs. 3-5; col. 8, lines 39-44) and video RAM in the video manager ("*non-volatile data storage module*"; For example see Fig. 5; col. 8, lines 51-63).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Boebert et al. (U.S.5,596,718), **Marino, Jr. et al.** (U.S.5,530,758) and **Holden et al.** (U.S.5,802,178) are all cited to show devices and methods for improving secure communications with trusted/untrusted networks in the telecommunication architectures, which are considered pertinent to the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tri H. Phan, whose telephone number is (571) 272-3074. The examiner can normally be reached on M-F (8:00-4:30).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chau T. Nguyen can be reached on (571) 272-3126.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

or faxed to:

(571) 273-8300

Hand-delivered responses should be brought to Randolph Building, 401 Dulany Street, Alexandria, VA 22314.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Technology Center 2600 Customer Service Office, whose telephone number is (571) 272-2600.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

BRIAN NGUYEN
PRIMARY EXAMINER

Tri H. Phan
June 27, 2005